

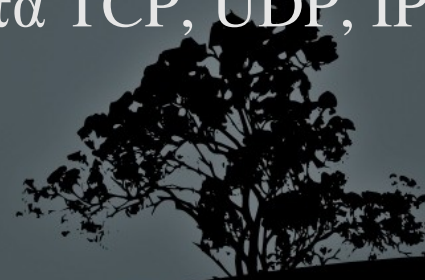
Εξέταση 102 – Μάθημα 14

109.1 Βασικές αρχές των πρωτοκόλλων διαδικτύου



Η σουίτα πρωτοκόλλων TCP/IP

- Το TCP/IP (Transport Control Protocol/Internet Protocol) είναι ένα σύνολο από πρωτόκολλα που χρησιμοποιούνται στο Διαδίκτυο αλλά και στα σύγχρονα τοπικά δίκτυα (LANs)
- Όλα τα σύγχρονα λειτουργικά συστήματα υλοποιούν την δική τους «στοίβα TCP/IP» (TCP/IP stack)
- Η στοίβα TCP/IP αποτελείται από 4 (κατά άλλους 5) επίπεδα (Εφαρμογών, Μεταφοράς, Διαδικτύου και Συνδέσμου)
- Κάθε ένα από τα πρωτόκολλα ανήκει σε διαφορετικό επίπεδο αλλά υπάρχουν και κάποια που ανήκουν σε δύο επίπεδα
- Βασικά πρωτόκολλα που θα εξετάσουμε είναι τα TCP, UDP, IP (IPv4, IPv6), ICMP και άλλα



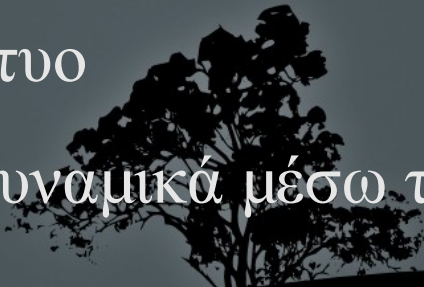
Το μοντέλο της στοίβας TCP/IP

Επίπεδο	Περιγραφή	Πρωτόκολλα
Εφαρμογών (Application)	Προσφέρει επικοινωνία μεταξύ δικτυακών εφαρμογών, διαχείριση συνεδριών (sessions) και παρουσίαση των δεδομένων με τρόπο κατανοητό	HTTP, SMTP, DNS, DHCP
Μεταφοράς (Transport)	Είναι υπεύθυνο για την μεταφορά των μηνυμάτων και διαχωρισμό των υπηρεσιών με την χρήση θυρών (ports). Προσφέρει έλεγχο σφαλμάτων, ρύθμιση ροής και κατάτμηση δεδομένων	TCP, UDP
Διαδικτύου (Internet)	Είναι υπεύθυνο για την δρομολόγηση των πακέτων δεδομένων σε ένα δίκτυο δικτύων (internetwork). Εδώ ορίζονται οι διευθύνσεις IP	IP (IPv4, IPv6), ICMP
Συνδέσμου (Link)	Είναι υπεύθυνο για την διαβίβαση των δεδομένων μεταξύ των φυσικών στοιχείων του δικτύου και δεν είναι κατακρίβειαν μέρος του TCP/IP	Ethernet, Wi-Fi, Token Ring, PPP, SLIP



Η δομή μιας διεύθυνσης IP (IPv4)

10101100000011110001100000000110 - 172.16.24.6

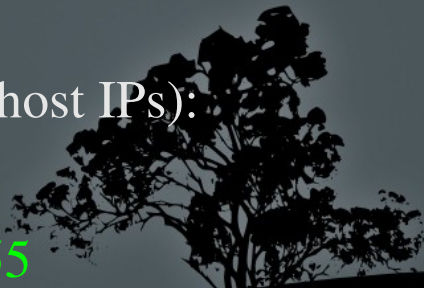
- Μια διεύθυνση IP αποτελείται από 32 δυαδικά μπιτ και αναπαριστάται με 4 οκτάδες σε δεκαδικό σύστημα με τον συμβολισμό διάστικτων δεκαδικών (dot-decimal notation).
 - Κάθε διεύθυνση είναι χωρισμένη σε δύο τμήματα:
 - **Τμήμα δικτύου**: καθορίζει το δίκτυο στο οποίο ανήκει η διεύθυνση
 - **Τμήμα κόμβου (host)**: καθορίζει την μοναδική ταυτότητα της συσκευής που χρησιμοποιεί το δίκτυο
 - Κάθε διεύθυνση είναι μοναδική σε κάθε δίκτυο
 - Οι διευθύνσεις ορίζονται είτε στατικά είτε δυναμικά μέσω του πρωτοκόλλου DHCP
- 

Διαχωρισμός δικτύων σε Κλάσεις Διευθύνσεων (Classes)

- Αρχικά ο διαχωρισμός σε δίκτυα γινόταν με τον καθορισμό κλάσεων

Κλάση	Αρχικά μπιτς	Μέγεθος τμήματος δικτύου (μπιτς)	Μέγεθος τμήματος κόμβου (μπιτς)	Αριθμός δικτύων	Διευθύνσεις ανά δίκτυο	Αρχική Διεύθυνση	Τελική Διεύθυνση
A	0	8	24	128 (2^7)	16.777.216 (2^{24})	0.0.0.0	127.255.255.255
B	10	16	16	16.384 (2^{14})	65.536 (2^{16})	128.0.0.0	191.255.255.255
C	110	24	8	2.097.152 (2^{21})	256 (2^8)	192.168.0.0	223.255.255.255
D	1110	N/A	N/A	N/A	N/A	224.0.0.0	239.255.255.255
E	1111	N/A	N/A	N/A	N/A	240.0.0.0	255.255.255.255

Παραδείγματα δικτύων Κλάσεων A, B και C

- **Κλάση A:** 86.0.0.0 – 86.255.255.255
 - Διεύθυνση δικτύου (network): 86.0.0.0
 - Χρησιμοποιήσιμες διευθύνσεις κόμβων (usable host IPs): 86.0.0.1 – 86.255.255.254
 - Διεύθυνση μετάδοσης (broadcast): 86.255.255.255
 - **Κλάση B:** 135.24.0.0 – 135.24.255.255
 - Διεύθυνση δικτύου (network): 135.24.0.0
 - Χρησιμοποιήσιμες διευθύνσεις κόμβων (usable host IPs): 135.24.0.1 – 135.24.255.254
 - Διεύθυνση μετάδοσης (broadcast): 135.24.255.255
 - **Κλάση C:** 215.25.17.0 – 215.25.17.255
 - Διεύθυνση δικτύου (network): 215.25.17.0
 - Χρησιμοποιήσιμες διευθύνσεις κόμβων (usable host IPs): 215.25.17.1 – 215.25.17.254
 - Διεύθυνση μετάδοσης (broadcast): 215.25.17.255
- 

Προβλήματα με το μοντέλο των Κλάσεων

- Αυτή η δομή βάση των κλάσεων δεν ήταν ιδανική.
- Ειδικά οι Κλάσεις A και B είχαν σπαταλήσει ένα μεγάλο μέρος από τον διαθέσιμο χώρο διευθύνσεων και οδηγηθήκαμε στην σημερινή έλλειψη διευθύνσεων IPv4
- Αυτά τα προκαθορισμένα μεγέθη δικτύων δεν εφαρμόζονταν σε όλους τους οργανισμούς γιατί ο καθένας έχει διαφορετικές ανάγκες
- Δεν είναι καλή πολιτική να μπαίνουν όλα τα τμήματα ενός οργανισμού κάτω από το ίδιο δίκτυο (προβλήματα επιδόσεων και ασφάλειας)



Διαχωρισμός δικτύων σε υποδίκτυα (subnetting) με την χρήση Μασκών

- Οι Μάσκες Υποδικτύων (Subnet Masks) είναι μια μέθοδος καλύτερου διαχωρισμού του διαθέσιμου χώρου διευθύνσεων σε μικρότερα δίκτυα
- Για να δημιουργήσουμε ένα υποδίκτυο δανειζόμαστε μπιτ από το τμήμα κόμβων για να μεγαλώσει το τμήμα δικτύου.
- Με αυτό το τρόπο δημιουργούμε περισσότερα υποδίκτυα από ένα κυρίως δίκτυο με μικρότερο αριθμό διαθέσιμων διευθύνσεων IP



Προκαθορισμένη Μάσκα για Κλάση A

- Η προκαθορισμένη Μάσκα για Κλάση A είναι:

255.0.0.0 = 11111111000000000000000000000000

- Εύρεση των ορίων ενός δικτύου Κλάσης A με την χρήση της προκαθορισμένης μάσκας πχ:

86.14.29.135

```
$ ipcalc 86.14.29.135 255.0.0.0
```

```
Address:    86.14.29.135      01010110. 00001110.00011101.10000111
Netmask:    255.0.0.0 = 8     11111111. 00000000.00000000.00000000
=>
Network:    86.0.0.0/8        01010110. 00000000.00000000.00000000
HostMin:    86.0.0.1          01010110. 00000000.00000000.00000001
HostMax:    86.255.255.254    01010110. 11111111.11111111.11111110
Broadcast:  86.255.255.255    01010110. 11111111.11111111.11111111
Hosts/Net:  16777214
```

Class A



Προκαθορισμένη Μάσκα για Κλάση B

- Η προκαθορισμένη Μάσκα για Κλάση B είναι:

255.255.0.0 = 11111111111111110000000000000000

- Εύρεση των ορίων ενός δικτύου Κλάσης B με την χρήση της προκαθορισμένης μάσκας πχ:

135.24.14.29

```
$ ipcalc 135.24.14.29 255.255.0.0
Address:   135.24.14.29           10000111.00011000. 00001110.00011101
Netmask:   255.255.0.0 = 16       11111111.11111111. 00000000.00000000
=>
Network:   135.24.0.0/16          10000111.00011000. 00000000.00000000
HostMin:   135.24.0.1             10000111.00011000. 00000000.00000001
HostMax:   135.24.255.254         10000111.00011000. 11111111.11111110
Broadcast: 135.24.255.255         10000111.00011000. 11111111.11111111
Hosts/Net: 65534                  Class B
```



Προκαθορισμένη Μάσκα για Κλάση C

- Η προκαθορισμένη Μάσκα για Κλάση C είναι:

255.255.255.0 = 1111111111111111111111111111111100000000

- Εύρεση των ορίων ενός δικτύου Κλάσης C με την χρήση της προκαθορισμένης μάσκας πχ:

215.25.17.45

```
$ ipcalc 215.25.17.45 255.255.255.0
Address:    215.25.17.45          11010111.00011001.00010001. 00101101
Netmask:    255.255.255.0 = 24    11111111.11111111.11111111. 00000000
=>
Network:    215.25.17.0/24       11010111.00011001.00010001. 00000000
HostMin:    215.25.17.1          11010111.00011001.00010001. 00000001
HostMax:    215.25.17.254        11010111.00011001.00010001. 11111110
Broadcast:  215.25.17.255        11010111.00011001.00010001. 11111111
Hosts/Net:  254                  Class C
```



Εύρεση των ορίων ενός υποδικτύου με διαφορετική Μάσκα

- Αν υποθέσουμε ότι έχουμε την εξής διεύθυνση:
215.25.17.45 με Μάσκα **255.255.255.192**

```
$ ipcalc 215.25.17.45 255.255.255.192
Address:    215.25.17.45          11010111.00011001.00010001.00 101101
Netmask:    255.255.255.192 = 26 11111111.11111111.11111111.11 000000
=>
Network:    215.25.17.0/26        11010111.00011001.00010001.00 000000
HostMin:    215.25.17.1          11010111.00011001.00010001.00 000001
HostMax:    215.25.17.62        11010111.00011001.00010001.00 111110
Broadcast:  215.25.17.63        11010111.00011001.00010001.00 111111
Hosts/Net:  62                   Class C
```

- Στην ουσία το δίκτυο **215.25.17.0/255.255.255.192**
είναι ένα υποδίκτυο του Κλάσεως C δικτύου
215.25.17.0/255.255.255.0

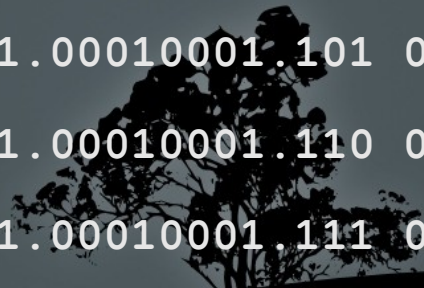


Εύρεση όλων των υποδικτύων ενός δικτύου Κλάσης

- Αν θέλουμε να χωρίσουμε το δίκτυο **215.25.17.0/255.255.255.0** σε υποδίκτυα με μάσκα **255.255.255.224** θα προκύψουν 8 υποδίκτυα:

```
$ ipcalc 215.25.17.0 255.255.255.0 255.255.255.224 | grep -A1 '[1-8]\\.\\$'
```

1.	Network:	215.25.17.0/27	11010111.00011001.00010001.000	00000
2.	Network:	215.25.17.32/27	11010111.00011001.00010001.001	00000
3.	Network:	215.25.17.64/27	11010111.00011001.00010001.010	00000
4.	Network:	215.25.17.96/27	11010111.00011001.00010001.011	00000
5.	Network:	215.25.17.128/27	11010111.00011001.00010001.100	00000
6.	Network:	215.25.17.160/27	11010111.00011001.00010001.101	00000
7.	Network:	215.25.17.192/27	11010111.00011001.00010001.110	00000
8.	Network:	215.25.17.224/27	11010111.00011001.00010001.111	00000



Διαχωρισμός δικτύου σε υποδίκτυα με διαφορετικές μάσκες

- Δεν είναι πάντα επιθυμητό να έχουμε τις ίδιες μάσκες στα υποδίκτυα μια και οι ανάγκες κάθε δικτύου σε διευθύνσεις μπορεί να είναι διαφορετικές. Πχ θέλω να διαχωρίσω το δίκτυο **215.25.17.0/255.255.255.0** σε άλλα υποδίκτυα με διαφορετικές μάσκες:

```
$ ipcalc 215.25.17.0 255.255.255.192 | egrep -i "(network|
broadcast)"
Network: 215.25.17.0/26          11010111.00011001.00010001.00 000000
Broadcast: 215.25.17.63        11010111.00011001.00010001.00 111111

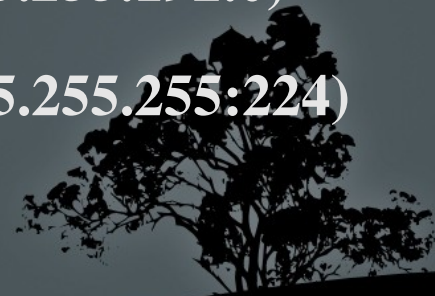
$ ipcalc 215.25.17.64 255.255.255.224 | egrep -i "(network|
broadcast)"
Network: 215.25.17.64/27        11010111.00011001.00010001.010 00000
Broadcast: 215.25.17.95        11010111.00011001.00010001.010 11111

$ ipcalc 215.25.17.96 255.255.255.224 | egrep -i "(network|
broadcast)"
Network: 215.25.17.96/27        11010111.00011001.00010001.011 00000
Broadcast: 215.25.17.127       11010111.00011001.00010001.011 11111

$ ipcalc 215.25.17.128 255.255.255.248 | egrep -i "(network|
broadcast)"
Network: 215.25.17.128/29       11010111.00011001.00010001.10000 000
Broadcast: 215.25.17.135       11010111.00011001.00010001.10000 111
```

Classless Inter-Domain Routing (CIDR)

- Τα προβλήματα με την λογική των Κλάσεων έγιναν εντονότερα και έτσι το IETF αποφάσισε να τις καταργήσει με την εισαγωγή του CIDR. Το CIDR εισήγαγε και καινούργιο συμβολισμό για τις Μάσκες το «Συμβολισμό CIDR» (CIDR notation). Σε αυτόν οι Μάσκες αναπαριστώνται με ένα αριθμό που ισούται με το αριθμών των “1” που περιέχουν, πχ: 255.255.255.0 -> /24
- Αυτή η καινούργια αναπαράσταση ονομάζεται δικτυακό πρόθεμα (network prefix). Κάποια παραδείγματα:
 - **215.25.17.0/24** (IP: 215.25.17.0 Μάσκα: 255.255.255.0)
 - **26.78.243.197/18** (IP: 26.78.243.197 Μάσκα: 255.255.192.0)
 - **212.165.7.168/27** (IP:212.165.7.168 Μάσκα: 255.255.255:224)



Ιδιωτικές Διευθύνσεις IP (Private IP Addresses)

- Λόγω της έλλειψης των διευθύνσεων διεθνώς δημιουργήθηκαν οι ιδιωτικές διευθύνσεις IP. Αυτές οι διευθύνσεις δεν είναι προσβάσιμες στο Διαδίκτυο και μπορούν να υπάρξουν μόνο σε εσωτερικά δίκτυα σε αντίθεση με τις δημόσιες διευθύνσεις (Public IP Addressess)
- Αν ένας υπολογιστής από ιδιωτικό δίκτυο επιθυμεί πρόσβαση στο Διαδίκτυο θα πρέπει η διεύθυνση του να «μεταφραστεί» σε μια δημόσια διεύθυνση IP μέσω ενός μηχανισμού «Μετάφρασης Δικτυακών Διευθύνσεων» (Network Address Translation) ή NAT.
- Κάθε ιδιωτικό δίκτυο με πρόσβαση στο Διαδίκτυο έχει μια ή περισσότερες δημόσιες διευθύνσεις IP. Οι εσωτερικές ιδιωτικές διευθύνσεις, οι οποίες είναι συνήθως πολύ περισσότερες από τις δημόσιες μεταφράζονται από κάποιο δρομολογητή (router) ή πυλώνα (gateway) σε δημόσιες.

Ιδιωτικές Διευθύνσεις IP (Private IP Addresses)

CIDR μπλοκ διευθύνσεων	Πεδίο διευθύνσεων	Αντιστοιχία σε δίκτυα Κλάσεων	Αριθμός διευθύνσεων
10.0.0.0/8 (255.0.0.0)	10.0.0.0 – 10.255.255.255	1 δίκτυο Κλάσης A	16.777.216
172.16.0.0/12 (255.240.0.0)	172.16.0.0 – 172.31.255.255	16 διαδοχικά δίκτυα Κλάσης B	1.048.576
192.168.0.0/16 (255.255.0.0)	192.168.0.0 – 192.168.255.255	256 διαδοχικά δίκτυα Κλάσης C	65.536




Το μέλλον: IPv6

- Η έκδοση 6 του IP (IPv6) δημιουργήθηκε με το για να απαλειφθεί το πρόβλημα της έλλειψης διευθύνσεων
- Εκτός από τις πολλές βελτιώσεις που εισάγει το σημαντικότερο είναι η χρήση 128 μπιτ που αντιστοιχεί σε ένα αστρονομικό αριθμό διευθύνσεων: $2^{128} = 3,4 \times 10^{38}$ διευθύνσεις
- Οι διευθύνσεις συμβολίζονται σε δεκαεξαδικό σύστημα και διαχωρίζονται με “:” σε λέξεις των 16 μπιτ, πχ:
- **2001:0db8:85a3:0000:0000:8a2e:0370:7334 ->**
2001:db8:85a3:0:0:8a2e:370:7334 ->
2001:db8:85a3::8a2e:370:7334
- **0:0:0:0:0:0:0:1 -> ::1** , **0:0:0:0:0:0:0:0 -> ::**
- **2001:db8:a::/64** (το /64 είναι το δικτυακό πρόθεμα σε CIDR)

Ειδικές διευθύνσεις

- **loopback:** Το δίκτυο Κλάσης A **127.0.0.0/8** χρησιμοποιείται μόνο για το έλεγχο της στοίβας TCP/IP. Η διεύθυνση **127.0.0.1** είναι ρυθμισμένη στην εικονική διεπαφή **lo** και το όνομα **localhost** αναλύεται στην διεύθυνση 127.0.0.1. Το δίκτυο 127.0.0.0/8 δεν μπορεί να χρησιμοποιηθεί για δρομολόγηση πακέτων ούτε στο Διαδίκτυο αλλά ούτε και σε εσωτερικά δίκτυα
- **link-local:** Οι διευθύνσεις **169.254.1.0** μέχρι **169.254.254.255** χρησιμοποιούνται για αυτόματη ρύθμιση του IP μιας δικτυακής κάρτας (πχ Ethernet) όταν δεν υπάρχει υπηρεσία DHCP στο δίκτυο. Οι κόμβοι με τα πιο πάνω IPs μπορούν να επικοινωνήσουν μόνο στο δίκτυο το οποίο βρίσκονται και μόνο με άλλα IP στο ίδιο πεδίο. Δεν μπορούν να επικοινωνήσουν εκτός του δικτύου στο οποίο είναι ενωμένοι

Πρωτόκολλα στο TCP/IP

- **IP (Πρωτόκολλο Διαδικτύου – Internet Protocol):** είναι το βασικότερο πρωτόκολλο του TCP/IP το οποίο χρησιμοποιείται από όλα τα υπόλοιπα.
 - Βασικό του καθήκον η μεταφορά πακέτων (δρομολόγηση - routing) δεδομένων από ένα δίκτυο σε άλλο με την χρήση διευθύνσεων IP.
 - Δεν παρέχει αξιοπιστία (unreliable),
 - Δεν παρέχει έλεγχο ροής (no flow control)
 - Είναι ασυνδεδειστροφές (connectionless)
 - Υλοποιείται στο επίπεδο Διαδικτύου
- 


Πρωτόκολλα στο TCP/IP

- **TCP (Πρωτόκολλο Ελέγχου Μετάδοσης – Transport Control Protocol):** Είναι το βασικότερο πρωτόκολλο για την δημιουργία συνδέσεων. Μεταφέρει δεδομένα μεταξύ εφαρμογών με την χρήση θυρών (ports)
 - Παρέχει αξιοπιστία (reliable)
 - Παρέχει Έλεγχο Ροής (flow control)
 - Είναι συνδεδεσιστρεφές (connection-oriented)
 - Είναι σχετικά αργό σε σύγκριση με το UDP
 - Υποστηρίζει μόνο μετάδοση **unicast** δηλαδή επικοινωνία μεταξύ δύο κόμβων
 - Υλοποιείται στο επίπεδο Μεταφοράς και χρησιμοποιεί το

Πρωτόκολλα στο TCP/IP

- **UDP (Πρωτόκολλο Διαγραμμάτων Χρήστη – User Datagram Protocol):** υλοποιείται στο επίπεδο μεταφοράς και όπως και το TCP χρησιμοποιεί τις θύρες (ports) για να στείλει τα διαγράμματα του
 - Δεν παρέχει αξιοπιστία (unreliable),
 - Δεν παρέχει έλεγχο ροής (no flow control)
 - Είναι ασυνδεδειστροφές (connectionless)
 - Είναι πιο γρήγορο από το TCP λόγω της απουσίας των πιο πάνω δυνατοτήτων
 - Υποστηρίζει unicast, broadcast και multicast
 - Υλοποιείται στο επίπεδο Μεταφοράς και χρησιμοποιεί το

Πρωτόκολλα στο TCP/IP

- **ICMP (Πρωτόκολλο Ελέγχου Μηνυμάτων Διαδικτύου – Internet Control Message Protocol):** χρησιμοποιείται για να ειδοποιεί τα υπόλοιπα πρωτόκολλα για την συμπεριφορά του δικτύου
 - Έλεγχος Ροής (flow control): ειδοποιεί το TCP αν υπάρχει συμφόρηση δεδομένων στο δίκτυο
 - Ειδοποιεί για απρόσιτους προορισμούς (Destination Unreachable)
 - Επαναδρομολόγηση διαδρομών (Route Redirection)
 - Έλεγχος απομακρυσμένων κόμβων πχ με την εντολή **ping**
 - Είναι ασυνδεδιστρεφές (connectionless)
 - Υλοποιείται στο επίπεδο Διαδικτύου και χρησιμοποιεί το **IP**
- 

Θύρες (Ports) και Υπηρεσίες

- Οι θύρες χρησιμοποιούνται στο επίπεδο μεταφοράς, από τα πρωτόκολλα **TCP** και **UDP**, για την ταυτοποίηση των υπηρεσιών σε ένα κόμβο
- Με λίγα λόγια για να μεταφερθεί ένα πακέτο δεδομένων χρειάζεται την διεύθυνση προορισμού του κόμβου και την ταυτότητα της υπηρεσίας για την οποία προορίζεται
- Ένας κόμβος μπορεί να προσφέρει πολλές υπηρεσίες οι οποίες διαχωρίζονται με διαφορετικές θύρες
- Οι υπηρεσίες υλοποιούνται στο επίπεδο Εφαρμογών ενώ οι θύρες στο επίπεδο Μεταφοράς
- Κάποια παραδείγματα υπηρεσιών: ftp, ssh, http, dns κτλ
- Το αρχείο `/etc/services` θα μας δώσει μια λίστα με υπηρεσίες και τις θύρες που χρησιμοποιούν

Κυριότερες Θύρες και Υπηρεσίες

Υπηρεσία	Θύρα(ες)	Περιγραφή
FTP (File Transfer Protocol)	20 (δεδομένα), 21 (έλεγχος)	Το πρωτόκολλο FTP χρησιμοποιεί το TCP για μεταφορά αρχείων
SSH (Secure Shell)	22	Ασφαλής σύνδεση σε άλλους κόμβους (TCP)
TELNET	23	Μη ασφαλής σύνδεση (!) σε άλλους κόμβους (TCP)
SMTP, SMTPS (Simple Mail Transfer Protocol)	25, 465 (SSL)	Αποστολή ηλεκτρονικής αλληλογραφίας (TCP)
DNS (Domain Name Service)	53	Επίλυση ονομάτων τομέα (domain names) σε διευθύνσεις IP (UDP/TCP)
DHCP	67 (Server), 68 (Client)	Αυτόματη ρύθμιση διευθύνσεων IP για όσους κόμβους το χρειάζονται (UDP)
HTTP/HTTPS (HyperText Transfer Protocol)	80, 443 (SSL)	Εξυπηρέτηση ιστοσελίδων – Παγκόσμιος Ιστός (TCP)
POP3, POP3S (Post Office Protocol)	110, 995 (SSL)	Παραλαβή αλληλογραφίας τοπικά (TCP)
NNTP (Network News Transfer Protocol)	119	Αποστολή/Παραλαβή δικτυακών ειδήσεων (newsgroups) (TCP)
Netbios	139	Πρωτόκολλο Netbios για δίκτυα Windows (UDP/TCP)
IMAP, IMAPS (Internet Message Access Protocol)	143, 993 (SSL)	Παραλαβή αλληλογραφίας σε διακομιστή (TCP)
SNMP (Simple Network Management Protocol)	161	Παρακολούθηση των επιδόσεων του δικτύου και των κόμβων καθώς και διαχείριση δικτύου (UDP/TCP)

Σύνδεση σε διακομιστές FTP με την εντολή *ftp*

- Η εντολή **ftp** είναι ένα «πελάτης» για σύνδεση σε διακομιστές **ftp** από γραμμή εντολών
- **# ftp ftp.debian.org #** σύνδεση ftp σε ftp.debian.org
- **# ftp -v ftp.debian.org #** σύνδεση ftp με αναλυτική προβολή
- Εντολές:
 - ftp> ls #** λίστα αρχείων/καταλόγων
 - ftp> cd dir #** είσοδος σε κατάλογο dir
 - ftp> get file #** λήψη αρχείου file
 - ftp> mget file[1-9] #** Λήψη αρχείων file1, file2, ..., file9
 - ftp> put file #** ανέβασμα αρχείου file από τοπικό τρέχον κατάλογο
 - ftp> mput file[a-f] #** ανέβασμα πολλαπλών αρχείων
 - ftp> pwd #** προβολή τρέχοντος καταλόγου σε διακομιστή
 - ftp> quit # = exit.** Διακοπή σύνδεσης με διακομιστή

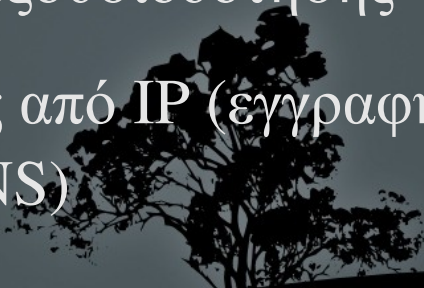
Σύνδεση σε κόμβους με γραμμή εντολών με *telnet*

- Η εντολή **telnet** χρησιμοποιούνταν στο παρελθόν για σύνδεση κελύφους σε απομακρυσμένους κόμβους. Λόγω της αδυναμίας του να στέλνει τα δεδομένα σύνδεσης, συμπεριλαμβανομένου και του κωδικού, σε καθαρό κείμενο έχει αντικατασταθεί από την εντολή **ssh** η οποία υποστηρίζει κρυπτογράφηση
- Χρησιμοποιείται επίσης για βασικό έλεγχο της λειτουργίας μη κρυπτογραφημένων πρωτοκόλλων πχ HTTP, SMTP κτλ
- **\$ telnet telehack.com #** σύνδεση με telehack.com
- **\$ telnet www.debian.org 80 #** σύνδεση με το διακομιστή ιστού της Debian για βασικό έλεγχο λειτουργίας
GET
- **\$ telnet mail-out.cytanet.com.cy 25 #** σύνδεση με το διακομιστή SMTP της Cytanet για βασικό έλεγχο λειτουργίας
quit
- **\$ telnet towel.blinkenlights.nl #** δοκιμάστε και θα δείτε! :)

Ερωτήματα σε διακομιστές DNS με *host*

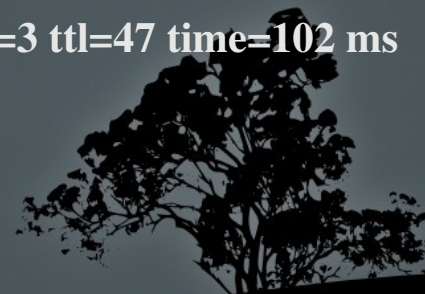
- Η εντολή **host** στέλνει ερωτήματα στους διακομιστές DNS
- **\$ host cut.ac.cy #** ερώτημα για εγγραφές A, CNAME (και MX αν υπάρχουν)
- **\$ host www.cut.ac.cy 8.8.8.8#** το ερώτημα να σταλεί στο DNS 8.8.8.8 αντί στο προκαθορισμένο DNS του συστήματος
- **\$ host google.com #** το google.com είναι εναλλακτικό όνομα (CNAME - alias)
- **\$ host -v google.com #** αναλυτική προβολή
- **\$ host -t SOA cut.ac.cy #** αναζήτηση του διακομιστή εξουσιοδότησης (authoritative server) για cut.ac.cy
- **\$ host -t NS cut.ac.cy #** αναζήτηση των διακομιστών DNS για cut.ac.cy

Ερωτήματα σε διακομιστές DNS με *dig*

- Η εντολή **dig** είναι ακόμη μια εντολή για ερωτήματα σε DNS
 - **\$ dig cut.ac.cy #** προβολή εγγραφών A, CNAME και NS
 - **\$ dig www.cut.ac.cy @8.8.8.8 #** το ερώτημα θα σταλεί στο DNS 8.8.8.8 αντί στο προκαθορισμένο DNS του συστήματος
 - **\$ dig www.google.com #** αυτό είναι CNAME (alias)
 - **\$ dig mx cut.ac.cy #** ερώτημα για διακομιστές αλληλογραφίας
 - **\$ dig ns cut.ac.cy #** ερώτημα για διακομιστές DNS
 - **\$ dig soa cut.ac.cy #** ερώτημα για διακομιστή εξουσιοδότησης
 - **\$ dig -x 87.228.200.143 #** αναζήτηση ονόματος από IP (εγγραφή PTR). Αντίστροφο DNS (Reverse DNS)
- 

Έλεγχος παρουσίας κόμβων με *ping*

- Η εντολή **ping** ελέγχει την ανταπόκριση δικτυακών κόμβων χρησιμοποιώντας το πρωτόκολλο **ICMP**.
- ```
$ ping 127.0.0.1 # έλεγχος της τοπικής στοίβας TCP/IP
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_req=1 ttl=64 time=0.031 ms
64 bytes from 127.0.0.1: icmp_req=2 ttl=64 time=0.051 ms
^C # Ctrl-C για να την τερματίσετε
--- 127.0.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.031/0.041/0.051/0.010 ms
```
- ```
$ ping www.google.com # έλεγχος ανταπόκρισης του www.google.com
PING www.l.google.com (173.194.69.147) 56(84) bytes of data.
64 bytes from bk-in-f147.1e100.net (173.194.69.147): icmp_req=1 ttl=47 time=100 ms
64 bytes from bk-in-f147.1e100.net (173.194.69.147): icmp_req=2 ttl=47 time=100 ms
64 bytes from bk-in-f147.1e100.net (173.194.69.147): icmp_req=3 ttl=47 time=102 ms
^C # Ctrl-C για να την τερματίσετε
--- www.l.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 100.609/101.233/102.330/0.820 ms
```



Έλεγχος παρουσίας κόμβων με *ping*

- `$ ping -c4 2.1.1.1 # αποστολή μόνο 4 πακέτων ICMP στο IP 2.1.1.1`
`PING 2.1.1.1 (2.1.1.1) 56(84) bytes of data.`
`# Δεν ανταποκρίνεται`
`--- 2.1.1.1 ping statistics ---`
`4 packets transmitted, 0 received, 100% packet loss, time 2999ms`
- `$ ping -c4 192.168.2.8 # αποστολή μόνο 4 πακέτων ICMP σε 192.168.2.8`
`PING 192.168.2.8 (192.168.2.8) 56(84) bytes of data.`
`From 192.168.2.11 icmp_seq=1 Destination Host Unreachable`
`From 192.168.2.11 icmp_seq=2 Destination Host Unreachable`
`From 192.168.2.11 icmp_seq=3 Destination Host Unreachable`
`From 192.168.2.11 icmp_seq=4 Destination Host Unreachable`
`# Απάντηση από κόμβο 192.168.2.11 ότι δεν είναι διαθέσιμο`
`--- 192.168.2.8 ping statistics ---`
`4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3013ms`
`pipe 3`

Έλεγχος διαδρομών με εντολές **traceroute** και **tracert**

- Οι εντολές αυτές χρησιμοποιούνται για να ελέγχουμε την διαδρομή μέχρι κάποιο κόμβο. Στα αποτελέσματα θα μας δείξουν τους ενδιάμεσους κόμβους και αν υπάρχει πρόβλημα θα ξέρουμε ακριβώς που βρίσκεται. Η **traceroute** έχει περισσότερες επιλογές από την **tracert** αλλά σε κάποιες διανομές δουλεύει μόνο για τον χρήστη **root**
- Η **tracert** είναι πιο καινούργια εντολή και σε κάποιες διανομές είναι προκαθορισμένη. Δουλεύει για όλους τους χρήστες
- Υπάρχει επίσης και η εντολή **mtr** που συνδυάζει τα αποτελέσματα των **traceroute/tracert** και του **ping** και συνεχίζει να δουλεύει μέχρι να πατήσουμε **Ctrl-C**



Έλεγχος διαδρομών με εντολές traceroute και tracepath

```
$ traceroute lilliput.theo-andreou.org
```

```
traceroute to lilliput.theo-andreou.org (31.170.110.53), 30 hops max, 60 byte packets
```

```
 1 192.168.2.1 (192.168.2.1) 1.974 ms 2.069 ms 2.241 ms
 2 gw.ip.primehome.com (46.21.57.254) 24.962 ms 25.094 ms 27.020 ms
 3 tshape-phome3-eth2.thunderworx.net (217.27.56.51) 27.274 ms 29.009 ms 29.157 ms
 4 r-psdl.lim.thunderworx.net (194.42.135.46) 30.794 ms 30.958 ms 32.280 ms
 5 j1.lim.thunderworx.net (46.21.53.205) 32.495 ms 34.197 ms 34.339 ms
 6 j1.lim.nsp-transit.net (78.158.134.250) 34.487 ms 21.688 ms 24.843 ms
 7 78.158.141.145 (78.158.141.145) 87.134 ms 87.231 ms 88.965 ms
 8 DE-CIX4.de.lambdanet.net (80.81.192.74) 90.074 ms 91.971 ms 92.205 ms
 9 DUS-1-eth000.de.lambdanet.net (217.71.96.65) 92.712 ms 92.917 ms 94.248 ms
10 switch-tec-FRA.de.lambdanet.net (217.71.107.138) 99.886 ms 101.141 ms 100.956 ms
11 m44001.wwwsrv.eu (31.170.106.124) 100.218 ms 100.387 ms 101.327 ms
12 31.170.110.53 (31.170.110.53) 86.029 ms 87.245 ms 85.426 ms
```



Έλεγχος διαδρομών με εντολές traceroute και tracepath

```
$ tracepath lilliput.theo-andreou.org
```

```
1: adm01lp614.local          0.214ms pmtu 1500
1: 192.168.2.1               1.098ms
1: 192.168.2.1               1.035ms
2: gw.ip.primehome.com       36.567ms asymm 3
3: tshape-phome3-eth2.thunderworx.net 37.443ms
4: r-psdl.lim.thunderworx.net 37.328ms asymm 3
5: j1.lim.thunderworx.net    37.045ms asymm 4
6: j1.lim.nsp-transit.net    36.791ms asymm 5
7: 78.158.141.145           99.056ms asymm 6
8: DE-CIX4.de.lambdanet.net  99.755ms asymm 7
9: DUS-1-eth000.de.lambdanet.net 99.457ms asymm 8
10: switch-tec-FRA.de.lambdanet.net 125.621ms
11: m44001.wwwsrv.eu        101.189ms
12: 31.170.110.53          100.398ms reached
```

```
Resume: pmtu 1500 hops 12 back 54
```

Αναζήτηση υπευθύνων για ονόματα τομέων και IPs με *whois*

- Η εντολή **whois** στέλνει ερωτήματα σε βάσεις δεδομένων οργανισμών εγγραφής ονομάτων τομέα και διευθύνσεων IP
- **\$ whois lpi.org #** αναζήτηση οργανισμού ή ατόμων πίσω από τον τομέα **lpi.org**
- **\$ whois 87.228.200.135 #** αναζήτηση οργανισμού ή ατόμων πίσω από το IP **87.228.200.135**
- **\$ whois cut.ac.cy #** δεν δουλεύει για τομείς **.cy!**

